Total Information Compliance:
The TIA's Burden Under The Wyden Amendment

A Preemptive Analysis of the Government's Proposed Super Surveillance Program

Prepared by

American Civil Liberties Union
Technology and Liberty Program

Monday, May 19, 2003

ACLU
AMERICAN CIVIL LIBERTIES UNION

Late last year, media reports began to surface on a secretive project underway at the Pentagon's main research wing, the Defense Advanced Research Projects Agency. The project, led by retired Admiral John Poindexter, a longstanding booster of high-tech intelligence gathering, carried the ominous moniker "Total Information Awareness."

As described in documents and statements by TIA officials, the program was an infrastructure for monitoring all transactions made by Americans in both government and corporate electronic databases around the world. It would be able to track every American's shopping habits, finances, travel plans, medical records, and many other activities – and then use complicated and questionable mathematical formulae to identify patterns that supposedly point to potential terrorist activity.

TIA became a magnet for criticism from across the political spectrum. Conservative talk radio hosts, concerned at the potential misuse of such a system by a left-leaning administration, joined with liberal pundits in demanding that TIA be abandoned. Others questioned the feasibility, practicality and cost of the system's stated mission. Conservative *New York Times* columnist William Safire called TIA a "super-snoop's dream."

In response to the widespread public outcry over TIA, members of Congress began to draft legislation that would put the brakes on the spy program. In January 2003, Congress passed a measure proposed by Sen. Ron Wyden (D-OR) that banned the use of TIA against Americans and prohibited further work on the program unless DARPA provided a report within 90 days containing:

- A "detailed explanation" of the program
- An assessment of the "likely efficacy" of TIA
- An assessment of the "likely impact" of TIA on "privacy and civil liberties"
- "A list of the laws and regulations that govern the information to be collected by" TIA

The government is expected to deliver its TIA report to Congress on or around May 20, and the first thing that Congress and the American people will need to evaluate is whether DARPA has adequately answered these questions.

There has been a great deal of confusion over the goals and mechanisms of the TIA program, much of it a result of seemingly contradictory statements issued by TIA officials themselves. But even after the most recent official description of the program, which was offered by DARPA Director Dr. Tony Tether in testimony before Congress on May 6, 2003, substantial questions remain.

This report was written by Jay Stanley, Communications Director of the Technology and Liberty Program of the ACLU.

What follows is an outline of the outstanding questions and issues we believe the report must address and answer in order to comply with Congress's directive.

1. A detailed explanation of the actual and intended use of funds

Before Americans can weigh the costs and benefits of the TIA program, they need clear answers about exactly what the program's limits and potentials are. Some confusion over TIA's capabilities stems from the fact that DARPA (as the agency constantly points out) is creating a tool, the use of which will fall to another agency or agencies. That means that DARPA cannot itself answer the question of how the system will be used. Rather, questions must be asked in terms of what the system is *capable* of doing.

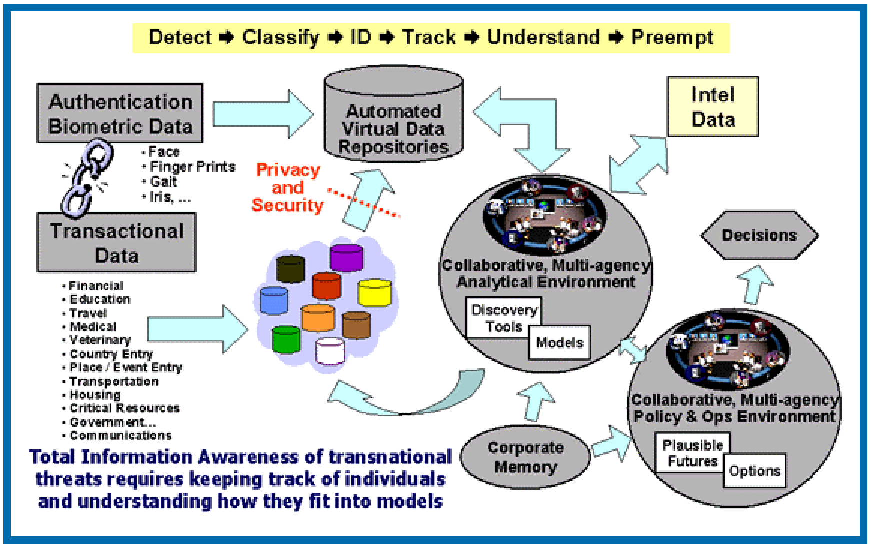
TIA's developers must supply definitive answers to the following questions about its operation:

A. Would the system be capable of connecting to and searching through an arbitrary number of distributed databases?
Will the number or composition of the databases accessed with TIA be in any way limited or hard-wired, or will the government agencies using the system have complete freedom to search as many databases of as many different types as they can legally access?

From a civil liberties perspective, this is a crucial question. If TIA can easily be scaled up to draw in more and more sources of data, then the technological path is clear for the program to turn into the all-encompassing surveillance tool that DARPA has denied it would become.

In his testimony, Dr. Tether denied that TIA planned to "use transaction data held by private companies." "I don't think we've ever said that," he said.[1] However, DARPA's own materials contain an extensive list of the categories of information planned for inclusion in the system (see chart). In addition, at the very same hearing where Dr. Tether spoke, a representative of the FBI admitted that "the FBI does utilize public source data." Given that it will be the FBI and other agencies and not DARPA that will actually deploy TIA, it is crucial that Congress be told what the system will be *capable* of searching, not just what DARPA with its ever-changing explanations now says.

[1] Testimony of Dr. Tony Tether before the House Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Committee on Government Reform, May 6, 2003. The comment quoted here was made during the question-and-answer portion of his testimony.


Detect ➔ Classify ➔ ID ➔ Track ➔ Understand ➔ Preempt
Authentication Biometric Data
• Face
• Finger Prints
• Gait
• Iris, ...
Transactional Data
• Financial
• Education
• Travel
• Medical
• Veterinary
• Country Entry
• Place / Event Entry
• Transportation
• Housing
• Critical Resources
• Government...
• Communications
Automated Virtual Data Repositories
Privacy and Security
Intel Data
Collaborative, Multi-agency Analytical Environment
Discovery Tools
Models
Decisions
Collaborative, Multi-agency Policy & Ops Environment
Plausible Futures
Options
Corporate Memory
Total Information Awareness of transnational threats requires keeping track of individuals and understanding how they fit into models

B. Would the system be capable of being used with a centralized database?
TIA officials have recently stressed that the system would be designed to work with scattered or distributed databases tied together, not a single centralized data repository. That seems to contradict earlier descriptions of the program, such as a chart describing the operation of the program that prominently features "automated virtual data repositories." That chart was featured on the TIA Web site and taken down after a firestorm of public outrage over the program erupted.

Of course, even if DARPA staff does not design TIA with a centralized database in mind, there is no reason why, once the product is finalized, that FBI agents or others elsewhere in government could not attempt to do so. Presumably, if the system can search through multiple databases, it should have no problem searching through a single database. Would TIA be *capable* of doing so, even if that is not how it is originally designed to be used?

C. What kinds of information analysis would the system be capable of?
Would TIA have the capacity to perform any kind of search for correlations or other statistical analysis, or other commonly used data-mining techniques (such as Exploratory Data Analysis, neural networks, etc.)? If not, could those capabilities, which involve highly intrusive searches through individuals' lives, be attached to the system at a later time?

In comments and documents made before the eruption of public outcry over TIA, program officials often seemed to suggest that this kind of data mining was what they had in mind. Admiral Poindexter, the head of TIA (and the most senior official implicated in the Reagan Administration's Iran-Contra scandal), told an audience in August 2002, for example, that "one of the significant new data sources that needs to be *mined* to *discover* and track terrorists is the transaction space."[2] Another top TIA official, Ted Senator, told the same audience that TIA was "all about" connecting information into "patterns that can be evaluated and analyzed, and learning what patterns discriminate between legitimate and suspicious behavior."[3]

One observer in a position to know what is going on in government is Gilman Louie, the head of In-Q-Tel, a venture capital fund established by the CIA. He says that the merits of data mining are the subject of "an ongoing argument" and "a big debate right now in government." [4]

DARPA says that it has been misunderstood. In his congressional testimony, Tether said that TIA will not involve sifting through everyone's information looking for models of what terrorist behavior might look like:

> When most people talk about "data mining," they are referring to the use of clever statistical techniques to comb through large amounts of data to discover previously unknown, but useful patterns for building predictive models. . . . DARPA is *not* pursuing these techniques.[5]

The TIA's actual approach, Tether, said, would be different:

> Our approach starts with developing attack scenarios. . . . These scenarios would be based on expert knowledge from previous terrorist attacks, intelligence analysis, new information about terrorist techniques, and/or from wargames in which clever people imagine ways to attack. . . .

The process he describes is one of query-based searches rather than data mining. "We create models, and say 'these would be the observables'" or behaviors that would be expected to flow from those models, the DARPA chief said. "We then take that pattern to the databases, and see if that pattern exists."[6]

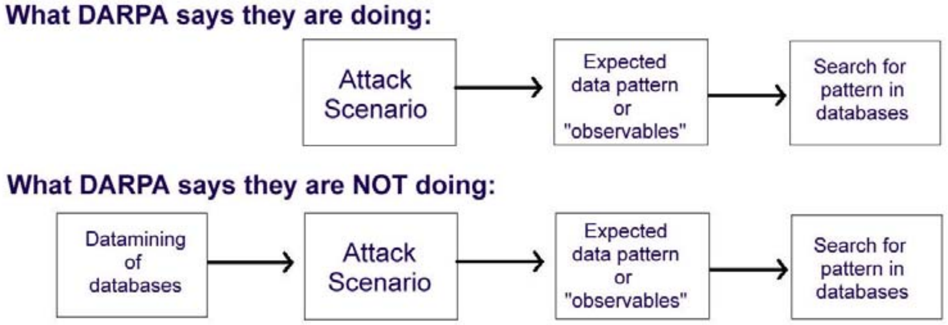
[2] Admiral John Poindexter, speaking at a DARPA conference in Anaheim, California, August 2, 2002. A copy of Poindexter's prepared remarks is online at http://www.fas.org/irp/agency/dod/poindexter.html.

[3] Senator is head of the "Evidence Extraction and Link Discovery Program" (EELD), a part of TIA. His comments are posted online at http://www.darpa.mil/DARPATech2002/presentation.html.

[4] Steve Lohr, "Data Expert is Cautious About Misuse of Information," *New York Times*, March 25, 2003.

[5] Written statement of Dr. Tony Tether submitted to the House Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Committee on Government Reform, May 6, 2003, pp. 1-2. Emphasis in original.

[6] Tether testimony, May 6, 2003. The comment quoted here was made during the question-and-answer portion of his testimony.


What DARPA says they are doing:
Attack Scenario
Expected data pattern or "observables"
Search for pattern in databases
What DARPA says they are NOT doing:
Datamining of databases
Attack Scenario
Expected data pattern or "observables"
Search for pattern in databases

Under both methods, the users of the TIA system would generate theories about what terrorists might be planning ("attack scenarios") and then search through databases looking for evidence of those theories. But when it comes to the question of how those attack scenarios will be generated, DARPA denies that it will be by an initial search through the databases for "suspicious patterns." Rather, they would be generated through intelligence analysis, "expert knowledge," and wargames in which clever people "imagine" possible attacks.

Whether TIA officials have changed the program's goals, have just put a new gloss on what they intend to do, or have been genuinely misunderstood from the beginning, is far from clear. But even if we accept DARPA's current, more modest description of what they are building, the program still appears to pose an enormous threat to Americans' privacy, and there are important questions about its operation that must be answered.

First, it is important to understand exactly how analysis of the TIA database will be conducted under real-world conditions. In truth, few data mining techniques involve trying to approach a set of numbers with no theories or models to test; there is always a complex interplay between theories and data. As creative and experimental analysts repeatedly ran, modified, and re-ran their attack scenarios through the TIA system, it would not be surprising if many of their searches began to resemble or duplicate the techniques used in data mining. Curious and aggressive agents will inevitably push the system to its hard-wired limits; it is important for Congress to be told what those limits will be.

Finally, the recognition by DARPA officials that a statistical analysis or data-mining strategy is (in Tether's words) "ill-suited to ferreting out terrorist plans" does not mean that it could not be tried at a later date by agents at the FBI or another agency that uses TIA, who might not possess the same understanding of the limits of data-mining. That is why it is important to establish the *capabilities* of the TIA system.

In the end, it is important to remember that every version of TIA that has been described, including pattern recognition, involves searching through billions of records about hundreds of millions of Americans.

2. The likely impact of TIA on privacy and civil liberties

By creating the means of combining together information on Americans' personal lives from many different sources into one rich view of their lives, the TIA program will bring into existence an immensely powerful surveillance tool. Like the atomic bomb, that tool will change the world just by being brought into existence, because it is so powerful that even if it is not used (or not used fully), the mere prospect of such use will change everyone's behavior. Given that reality, there are numerous questions that must be answered in fulfilling Congress's request for an assessment of the program's impact on privacy and civil liberties.

A. What difference would a distributed database make?
TIA officials have recently been touting the fact that the system would be based on distributed databases, and not one large central compendium of information, as a reason not to worry about the program. In today's world that is a distinction without a difference. Communications technologies like the Internet now make it possible to build a system for searching multiple databases all over the world that is, from the user's perspective, completely indistinguishable from searching a single, local, centralized database. (Millions of people experience that phenomenon every day when they use Internet search engines like Google.) Admiral Poindexter was referring to this fact when he declared that TIA's goal is to "develop ways of treating the world-wide, distributed, legacy databases as if they were one centralized database."[7]

The difference between centralized and distributed databases is invisible to the user, and makes no difference for privacy. No matter what the database architecture, the important thing is what information is available to the users. If anything, a distributed architecture appears to make possible far more powerful and up-to-date database than would a centralized repository. TIA needs to answer the question of how a distributed database would benefit privacy and civil liberties, or acknowledge that the distinction is irrelevant.

B. How can Americans be free when their every move is open to potential scrutiny?
As many a suspicious employer knows, individuals are just as affected by the knowledge that we *might be* under observation as we are by the *certainty* that we're being watched. When you don't know whether or not you're being monitored, the safe thing to do is to act as if you are at all times. Even under the more restrictive, query-based version of TIA, it will always be possible that our innocent activities will coincide with the latest imaginative "threat scenario" being explored at TIA Central, placing us under a microscope.

When every recorded activity in which Americans participate becomes subject to potential review by federal agents, American life, always distinguished by its open, free-wheeling nature, will fall under a cloud. Clearly, Americans don't want everything they do watched by the government. DARPA needs to address the issue of how TIA can be

[7] Poindexter, Anaheim, Calif., August 2, 2002.

implemented without violating that principle given the fact that potential monitoring is just as potent a source of control as actual monitoring.

C. What are the limits of privacy-enhancing technologies?

Imagine that the government set up computers that recorded every telephone call made in the country, converted the audio signals to text, and analyzed their contents without disclosing them to any human beings. The computer then alerted the authorities to any conversations that matched descriptions of "threat scenarios" entered by government security agents. Or, imagine that the government installed video cameras throughout every home in the country, and fed the video images to a computer, which analyzed the images and recorded descriptions of the behavior it observed, again without disclosing anything to the authorities.

Even if the authorities had to get a warrant in this scenario to access our information and discover our identity (and most of the data TIA would search could be obtained without one), all the bad effects that come from government spying would be felt: feelings of being monitored, a restricted sense of freedom, a chilling of free speech (especially speech critical of the government), and potential abuses of power. Even if the records of our every move and our every conversation were "anonymized" by special privacy-protecting technologies but could still be perused by agents testing their latest imaginative threat scenario, we would no longer be free. In effect, a government informant would be listening to every call and watching our every move, constantly prepared to call us to the attention of the authorities. The fact that that informant is a computer would be of little comfort (and might even be worse).

TIA, in essence, is a proposal to set up a system to do just this. Although it would spy on our transactions rather than our conversations and our behavior in the home, the information assembled by TIA would offer a view into our lives that would be scarcely less intrusive – especially as the cloud of transactional information captured about each of us continues to thicken. And the simple fact is that there are no real legal impediments to the government gaining access, through purchase and cooperative disclosure, to virtually all of the "transaction space."

Although our imaginary video and telephone-monitoring system would not be possible under current interpretations of the Constitution, the American legal system has not yet had a chance to extend those interpretations to cover the transactional information that would be assembled by a TIA system. The builders of TIA propose to exploit this growing gap in our privacy protections and build permanent institutions around it.

D. How can the bedrock Anglo-American principle of "individualized suspicion" be maintained?

It has always been a core principle of the American legal tradition that the government is not allowed to spy on you unless it has *individualized suspicion* that you are involved in wrongdoing. The government is not allowed to spy on you as part of a broad fishing expedition, or because you are a prominent (or not-so-prominent) member of the Republican party, the Democratic party, the ACLU, or the Eagle Forum. DARPA needs to explain how the principle of individualized suspicion can be squared with a system that:

- **Exposes every American to the possibility of having all their transactions scrutinized by the government.** That exposure would take place on no basis other than the fact that a person's activities happen to coincide with a speculative scenario for possible terrorist activity dreamed up by a government security agent.
- **Effectively asks every American a specific question about their life every time the system is searched.** For example, if a security agent were to come up with a model that includes people who have recently purchased several garden hoses, the TIA system would then have to search its database for people who fit that description. It would do so by examining *every person* in the database, and looking to see whether they have recently purchased garden hoses. That means that every time a query is run, a person is, in effect, being asked a question about their life by the government. Except that that query takes place in secret; looks at data that an individual might not even be aware has been collected about them; and leaves the individual no leeway in how the question is answered and no chance to explain away the presence of any flukes, errors, or unusual circumstances.

E. How will TIA likely affect privacy and civil liberties over time?

DARPA's assessment of the civil liberties implications of TIA must examine not just how TIA is likely to operate the day after it is turned on, but how it is likely to evolve over time given certain well-observed tendencies that are found in governments and in human beings across time. Its analysis must be diachronic (concerned with how something changes through time) rather than synchronic (concerned with how something appears frozen at one moment in time).

In particular, what are the likely implications of TIA in light of certain time-tested historical realities:

- The tendency for government agencies to expand and not contract in size and power. As TIA grows, will it form a powerful bureaucratic lobby for increased surveillance in American life?
- The tendency of information systems to grow, not only in the data they collect, but in the uses to which they are put. Once the system is in place, will its operators grow frustrated at the gaps in its coverage, and seek to have more and more transaction records available to them? Will TIA be expanded from terrorists to murderers to thieves, and so on down the scale of wrongdoing until everyone is put on guard against the slightest infraction of every law, rule, regulation, and social code in America? Since no wrongdoing, however small, is truly defensible, at what point will the nation draw the line?
- The tendency for law-enforcement and other government agencies to find their mission twisted from time to time by their political overseers toward political ends.
- The occasional emergence of periods in American history of intense social and political conflict, such as the Vietnam anti-war and Civil Rights movements and the

labor movement earlier in the century – and the intense fear of terrorism that we are now experiencing.

- The tendency of law enforcement agencies and personnel to take sides in those conflicts.

Even if we accept the premise that it would be possible to build a perfect system that allowed government agents to browse through records of individuals' activities under a regime of unimpeachably watertight privacy protections (although neither the technology nor the privacy laws for such a regime now exist), how long would such a system be likely to remain watertight under the immense pressures to which it will be subjected over time?

Build a system for perfect surveillance and they will come.

The American founding fathers took a long-range perspective when they set up our democracy. Even though everyone knew that perhaps the most trusted man in the nation – George Washington – was going to be president, the founders still set up a system of government based on checks and balances. They knew that temptations and attempts to abuse power were, over time, inevitable – and because the Constitution they drew up incorporated that recognition, the United States has been for 200 years the world's most stable democracy.

Our Constitution was built to last, and policymakers today contemplating surveillance systems with a potentially revolutionary impact on American life have a responsibility not to cast aside that wisdom and install the seeds of an institution that will corrode our freedom, either suddenly or over time.

3. The likely efficacy of TIA

Serious questions have been asked about the likely efficacy of TIA. Given the substantial civil liberties implications of TIA, DARPA must meet a very high standard in demonstrating its likely effectiveness in catching terrorists and saving lives.

Gilman Louie, the head of In-Q-Tel, said in March that he thought that the data mining approach is too blunt an instrument to be a primary tool of surveillance. "I think it's very dangerous to give the government total access," he said.[8] The Association for Computing Machinery has also expressed serious doubts about the program's feasibility:

> The overall surveillance goals of TIA suffer from fundamental flaws that are based in exceedingly complex and intractable issues of human nature, economics and law. . . . As computer scientists and engineers we have significant doubts that

[8] Steve Lohr, "Data Expert is Cautious About Misuse of Information," *New York Times*, March 25, 2003.

> the computer-based TIA Program will achieve its stated goal of "countering terrorism through prevention."[9]

DARPA has always traditionally tackled research tasks that are extremely difficult and futuristic in nature – an often-celebrated quality that has even led to projects of uncertain feasibility being called "DARPA-hard." While such boldness may be admirable in many cases (such as language translation), the calculus is different when it comes to projects with enormous social and political implications. In the case of TIA, where the intrusion on privacy is virtually certain, the slim chance of success places a heavy burden on DARPA to demonstrate the benefits of its project. After all, it is entirely possible that TIA would lead to dangerous invasions of privacy while still failing as a means of stopping terrorism. At the very least, DARPA must address several key questions that have been raised by observers about the feasibility of the TIA concept:

How bad will the problem of false positives be?

Given that there are approximately 300 million residents of the United States, and in all probability no more than a handful of persons planning terrorist attacks, the question of how many people will be falsely flagged or accused of being a potential terrorist by a system like TIA is a vital one.

The consequences of being falsely singled out as a potential terrorist can range from having one's privacy invaded, to enduring inconvenient and humiliating security checks, to damage to career or reputation, harmful notations in one's record, to arrest and imprisonment. Already since the 9/11 terrorist attacks, we have witnessed the damage that such accusations can do. Many immigrants were unfairly imprisoned, often for months at a time. The FBI under its "Project Lookout" gave corporations a list of hundreds of names of people it sought in connection with September 11. The list, which was riddled with inaccuracies and contained the names of many people the Bureau simply wanted to talk to, was widely circulated and took on a life of its own. No one knows how many innocent people have been denied jobs or suffered other harm because of the list.[10] And the government's "no-fly" list of terrorist suspects has been a similar disaster, ensnaring hundreds of innocent Americans who find themselves facing intense security scrutiny every time they fly, with no way of finding out how they got on a list or how to get off.[11]

As a little simple math shows, even a system that is 99% accurate will generate disabling numbers of false positives under a data mining system. The population of the US is about 300 million. If we assume that there are an additional 1,000 terrorists living here, a 99% accurate system would catch 990 of them. But it would also flag 3 million innocent

[9] Association for Computing Machinery Public Policy Committee, letter to Sens. John Warner and Carl Levin, January 23, 2003. Available online at http://www.acm.org/usacm/Letters/tia_final.html.

[10] Ann Davis, "Far Afield: FBI's Post-Sept. 11 'Watch List' Mutates, Acquires Life of Its Own," *Wall Street Journal*, Nov. 19, 2002.

[11] An ACLU press release on the case is online at http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=12439&c=206. In addition, the Electronic Privacy Information Center has posted hundreds of complaints filed by passengers at http://www.epic.org/privacy/airtravel/foia/watchlist_foia_analysis.html.

Americans as terrorists. That would leave a total of 3,000,990 people who have been identified as terrorists – and of course the authorities won't know which among them are the real terrorists.[12] The amount of investigative effort that would be involved in winnowing that field would be staggering. More realistic assumptions show even more dysfunctional ratios of real catches to false alarms.

Number of non-terrorists living in US	300,000,000	300,000,000	300,000,000
Number of terrorists living in US	1,000	1,000	1,000
Accuracy in identifying terrorists as terrorists	99.99%	99.00%	50.00%
Accuracy at identifying innocent as innocent	99.99%	99.00%	97.00%
# of terrorists who will be caught	1,000	990	500
# of innocent people who will be "caught"	30,000	3,000,000	9,000,000
Total # of people flagged as "terrorists"	**31,000**	**3,000,990**	**9,000,500**
Of those, number who really are	**1,000**	**990**	**500**

In short, this kind of a system rapidly becomes useless unless extremely high levels of accuracy can be maintained – levels that are, in fact, completely unrealistic.

We are told that the problem of false positives would be less severe on a system that is based on scenarios generated by analysts rather than scenarios generated through statistical analysis or data mining. But that assumes that the scenarios are themselves going to be accurate. Given the creativity of both terrorists and the analysts trying to anticipate their attacks, the number of "threat scenarios" that could be imagined is nearly infinite. In addition, many attacks could be imagined that involve transactions that are extremely common and match the activities of hundreds of thousands or even millions of people.

How much behavior would the system have to monitor to be effective?
Even if it is installed to the maximum extent, the TIA system would only be able to search and analyze those activities that leave behind electronic records. Electronic transactions that are not stored in databases, cash or paper transactions, and illegal or black-market activities would not leave traces in the searchable "transaction space" and so would not be covered by any queries launched by TIA operators.

Ironically, activities that leave no or fewer trails are precisely the sort of transactions that real terrorists, who strive to live "below the radar," will engage in. TIA could easily be the kind of system that sweeps up the innocent rather than the guilty.

[12] This problem has been pointed out by several experts, including computer scientist Benjamin Kuipers of the University of Texas at Austin, analysis online at http://www.interesting-people.org/archives/interesting-people/200212/msg00061.html and Bruce Schneier, http://www.counterpane.com/crypto-gram-0304.html.

That point is crucial because unfortunately what is likely to happen is that the information available to the TIA's computers, while representing an enormous amount of data about Americans' personal lives, will not be enough to fully explore the threat scenarios dreamed up by security agents. The result will be that the institutions that operate the TIA system will work to envelop more and more sources of information into the system, and push public officials to expand the kinds of information that they can legally include.

4. The laws and regulations that govern TIA

Congress has asked DARPA to survey the existing laws and regulations that would govern the TIA program. That is an important exercise, but it is largely irrelevant to the larger policy questions raised by the TIA program. That is because current privacy laws largely don't cover government access to the kind of third-party transactional information – financial, medical, education, travel, transportation, housing, communications – that TIA envisions using.

Medical information, for example, is subject to a complex new set of privacy regulations, but those regulations (known by the acronym HIPAA) permit broad access by law enforcement to patients' records. In another example, the FBI reportedly has an $8 million contract allows government agents to tap into the data aggregator Choicepoint's vast database of personal information on individuals.[13] Although the Privacy Act of 1974 banned the government from maintaining information on citizens who are not the targets of investigations, the FBI can now evade that requirement by simply purchasing information that has been collected by the private sector.

TIA officials are fond of emphasizing that their program "will comply with all the current privacy laws." But the reason that TIA is such a fiercely debated topic is precisely that the laws in this area have been totally outstripped by technology. The law didn't anticipate several factors that have emerged in recent years:

1. **The growing collection of information in private databases.** With the use of computer chips in everything from car and office keys to cell phones to transit passes, and with the private sector's discovery that it is very profitable to gather, analyze, and sell information on customers, more and more information is being collected about more and more of our activities.
2. **The ability to conduct mass sweeps through data.** Until recently our privacy has been protected by the fact that it was difficult or impossible to bring together information about individuals collected by different parties at different times and places. Searching for information across different databases used to be a cumbersome, time-consuming process. But today the Internet allows for the instantaneous sharing of databases that once would have had to be copied onto tape reels and physically shipped. And the increasing standardization of data

[13] Glenn R. Simpson, "Big Brother-in-Law: If the FBI Hopes to Get The Goods on You, It May Ask ChoicePoint" Wall St. Journal, April 13, 2001.

formats as well as advances in database-merging technology makes information increasingly easier to compare.

3. **The emergence of distributed databases.** As discussed above, the distinction that has been built into our privacy laws between information that the government itself "maintains" and information held by others that is open for the government to *access*, is now obsolete.

A delicate and careful balance has been constructed in American life between individuals' right to privacy and the government's right, in some situations, to spy on people. Initially set by the Constitution's Fourth Amendment, that balance has been readjusted over the years in response to new technologies ranging from the telephone to thermal imaging devices. Often, it took the courts many years to adjust to new technologies – telephone conversations, for example, were not folded under the Fourth Amendment for several decades.

One can hope that eventually our legal system will extend privacy protections to fill in the gaps created by these developments. But the Total Information Awareness program and the technologies behind it – new ways of collecting, storing, and assimilating information about Americans' daily activities – would rush into the current gap created by the law's lag behind technology, and create powerful institutions with a vested interest in maintaining and expanding that gap. The simple fact is that the technology is developing at the speed of light, while the law crawls along at a tortoise's pace. TIA or its equivalent could be the perfect storm of surveillance from which we have no shelter.